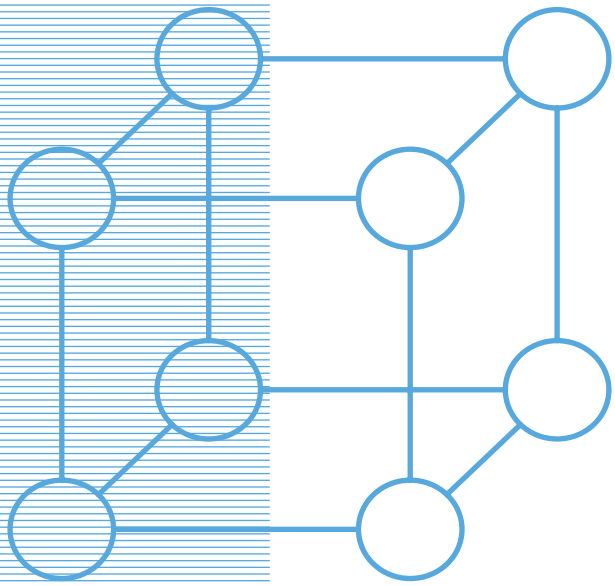
PD6 Exh 20

A Maturity Model for Integrated GRC



Sponsored by

RSA

OCEG®

August 2016

OCEG is a global, nonprofit think tank and community. We invented GRC.

We inform, empower and help advance more than 50,000 members on governance, risk management, and compliance (GRC). Independent of specific professions, we provide content, best practices, education, and certifications to drive leadership and business strategy through the application of the OCEG GRC Capability Model and Principled Performance. An OCEG differentiator, Principled Performance enables the reliable achievement of objectives while addressing uncertainty and acting with integrity.

Our members include c-suite, executive, management, and other professionals from small and midsize businesses, international corporations, nonprofits, and government agencies.

Founded in 2002, OCEG is headquartered in Phoenix, Arizona. For more information visit www.oceg.org.

RSA's Intelligence Driven Security solutions help organizations reduce the risks of operating in a digital world. By improving visibility, analysis and action, RSA solutions give customers the ability to prevent, detect, investigate and respond to IP theft, fraud and cybercrime.

RSA Archer's vision is to help organizations transform compliance, manage risk and exploit opportunity with Risk Intelligence made possible via an integrated, coordinated GRC program. The RSA Archer Maturity Model series outlines multiple segments of risk management that organizations must address to transform their GRC programs.

RSA Archer Maturity Models typically focus on key capabilities enabled by the RSA Archer solutions. For the Integrated GRC Maturity Model presented here, RSA analyzed best practices in some of its largest implementations to gain insight into what it takes to implement an integrated GRC program. You can find other RSA maturity models at https://www.rsa.com/en-us/perspectives/resources.

Table of Contents

Introduction

As the think tank that defined the business concept of GRC, OCEG has long talked about the need for a harmonized set of capabilities that enable an organization to reliably achieve its objectives, while addressing uncertainty and acting with integrity. These capabilities are outlined in the GRC Capability Model ("the OCEG Red Book"), the publicly vetted, free and open source standards for GRC planning and execution. The outcome of applying effective GRC is Principled Performance, which demands a mature, integrative approach to governance, risk management and compliance; the component parts of GRC.

Over the past 12 years, since the first release of the OCEG Red Book, organizations of all types and sizes, and in countries all over the world, have embraced the concept of integrated GRC. They have, at various speeds and starting points, evolved their GRC capabilities in organizational structure, processes and technologies.

Yet, many questions remain:

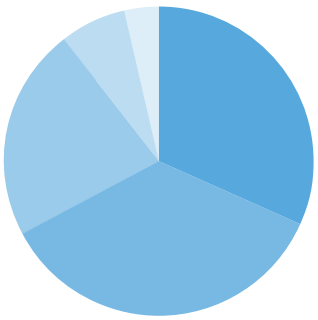
- What represents GRC maturity?
- What are the stages that we must pass through to establish GRC capabilities that truly support the business?
- Do the stages of GRC maturity mean the same capabilities are put in place for every organization?
- What business benefits do we gain from maturing GRC?

To address these questions, RSA Archer, an OCEG GRC Solutions Council member and a leader in GRC technology, has developed the Maturity Model for Integrated GRC drawing from the real world experience of some of its largest users.

We are pleased to share the details of the Maturity Model for Integrated GRC in this eBook, which discusses ways that GRC structures, practices and technologies change as maturity for GRC capability grows. In its pages you will find ways to describe the benefits your organization will gain as you mature your own GRC capabilities to leverage processes, share data and streamline efforts. Use this information to make the business case for starting or continuing movement from siloed reactive, compliance-driven processes to an integrated risk-centric, GRC program in your organization.

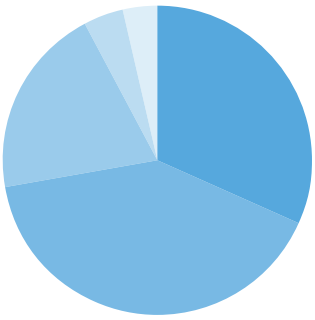
The trend toward greater GRC maturity overall is easy to see. OCEG recently conducted a poll of 100 GRC in-house professionals primarily in risk, compliance, internal audit and IT roles. Based on the Integrated GRC Maturity Model scale described in this eBook, more than two-thirds of the participants indicate that their organizations are on the journey to greater GRC maturity.

What best describes the maturity of your organization's current GRC capabilities?



- Siloed 32.8%
- Transitioning..... 35.3%
- Managed..... 21.8%
- Transforming..... 6.7%
- Advantaged 3.4%

How would you describe - your organization's GRC capabilities?



- Departmentalized 31.9%
- Becoming Standardized ... 41.2%
- Standardized and Well Managed 19.3%
- Supporting the Business with GRC 4.2%
- Harnessing Risk to Exploit Opportunities 3.4%

Nearly a quarter report that they have achieved the "Managed" state of maturity, in which core GRC processes are well defined and reporting is standardized. More than another 10% are either transitioning toward or report they have achieved "Advantaged" GRC with optimized processes and the ability to provide true support for business objectives.

When asked about maturity from the perspective of outcomes, we see that those who are at - or transforming toward - the Advantaged state have moved beyond standardized and well-managed GRC processes and now can harness risk to exploit opportunities in ways that truly support the business while addressing threats and ensuring compliance. This is Principled Performance and it is achieved through greater GRC maturity.

As this eBook describes, there are four core aspects to GRC capabilities that must all be addressed to grow GRC maturity.

- Organizational and governance structures must be defined to establish ownership, reporting and communication and to ensure appropriate resources are applied.
- Risk and compliance culture must begin with clearly established views, tolerances and guidance from senior management and continue with ongoing education and awareness at every level from management through front line employees.
- GRC program management must mirror business operations management, with established goals and performance indicators supported by efficient and well-executed strategic plans.
- GRC technology must be designed and architected as a process and data engine to support GRC programs and provide risk-aware information to business managers and strategic planners for the organization.

As you use this eBook to better understand the stages of the Integrated GRC Maturity Model, consider where your organization falls on the scale today, both across the enterprise and unit by unit.

Evaluate the areas where you might act first to gain the most value and where your defined risk profile calls for change.

Finally, as you develop your workplan for further stages of maturation, remember to always recall the goal of Principled Performance and determine what is needed to ensure that your organization can reliably achieve its objectives while addressing uncertainty and acting with integrity.

We hope you find this eBook useful as you map your own journey to maturing Integrated GRC.

The OCEG Executive Team

Why Integrated GRC?

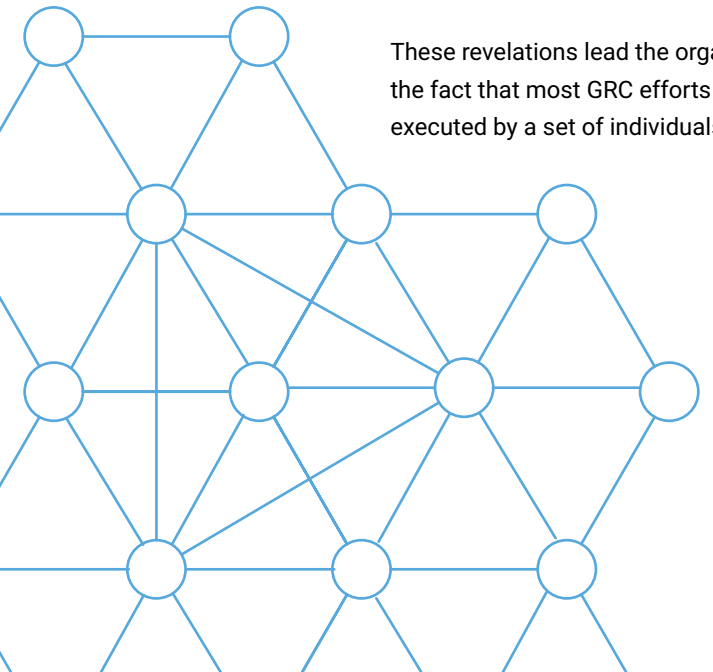
Most often, Governance, Risk and Compliance (GRC) efforts begin as a focused attempt to improve certain elements of risk or compliance management within one functional area such as IT, security or finance.

The function takes on the challenge of building a defined approach to methodically review risk, or catalog compliance obligations, to ensure that this individual piece of the organization is properly tracking towards its objectives. The drivers for this effort can be many – regulatory pressure from an external entity, strategic acknowledgment by executives or bottom up efforts by front line managers to reduce risks. Eventually, this function designates resources, implements processes and utilizes some technologies to address risk and compliance issues.

As more functions understand that risk and compliance management is part of managing business operations, more GRC efforts are created. Most organizations take the path of building individual pieces of the overall GRC program independently as each function has its own nuances and challenges. As GRC implementations become more mature, the organization realizes there are significant benefits to streamlining processes, reducing efforts and eliminating redundant activities.

These revelations lead the organization to address the fact that most GRC efforts are generally executed by a set of individuals tasked with managing risk and compliance processes, now often referred to as the Second (2nd) Line of Defense (LoD). The First (1st) LoD consists of the frontline employees and business managers closest to the risks within the business. Many times, the 1st LoD have conflicting or redundant requirements placed on them by different functional GRC efforts. Integrated GRC reduces this complexity for business operations through combined or coordinated efforts by the 2nd LoD. In other words, Integrated GRC can make the 2nd LoD more effective through shared processes and data and the 1st LoD more efficient through streamlined and prioritized efforts.

An Integrated GRC program breaks down silos between functional areas and enables common processes, taxonomies and technology infrastructure to both streamline risk and compliance efforts and build a risk aware organization. The cultural impact of an integrated program can be tremendous. The organization sees managing risk as a key ingredient of the success of the business – not as a deterring obstacle for progress. Getting to the level of maturity of an Integrated GRC program is a matter of constantly expanding, communicating, exploring and evolving.



Key Capabilities

Integrated GRC differentiates between GRC efforts that are singly focused on one dimension of risk and GRC efforts that are driven by a single view or strategy that bridges multiple functions. The term 'integrated' is used to describe the interconnection and communication between GRC functions rather than meaning a consolidated, centralized function. Every GRC initiative will have its own distinctive traits. However, there are some common elements that can be leveraged across functions that will improve the overall effectiveness of the risk and compliance efforts as well as reduce costs and build efficiencies.

When an executive team seeks to assemble an enterprise (integrated) program for risk and compliance, multiple operational groups are required to collaborate and coordinate efforts to achieve these specific goals:

- Clear ownership and communication channels must be established to provide oversight and accountability.
- The strategic vision must be implemented such that roles, responsibilities and objectives filter down to the front line employees to ensure consistency across risk and compliance efforts.
- GRC efforts must be coordinated ensuring risk and compliance initiatives are executed in the context of the broader strategy.
- Technology must be harnessed to full effect for it to be a true enabler for GRC.

To achieve these goals, RSA Archer's Integrated GRC Maturity Model focuses on the following key capabilities:

Establish organizational and governance structures

Enable the various functional groups to understand the program's ownership and accountability models and lay the foundation for clear coordination and communication.

Build risk and compliance culture

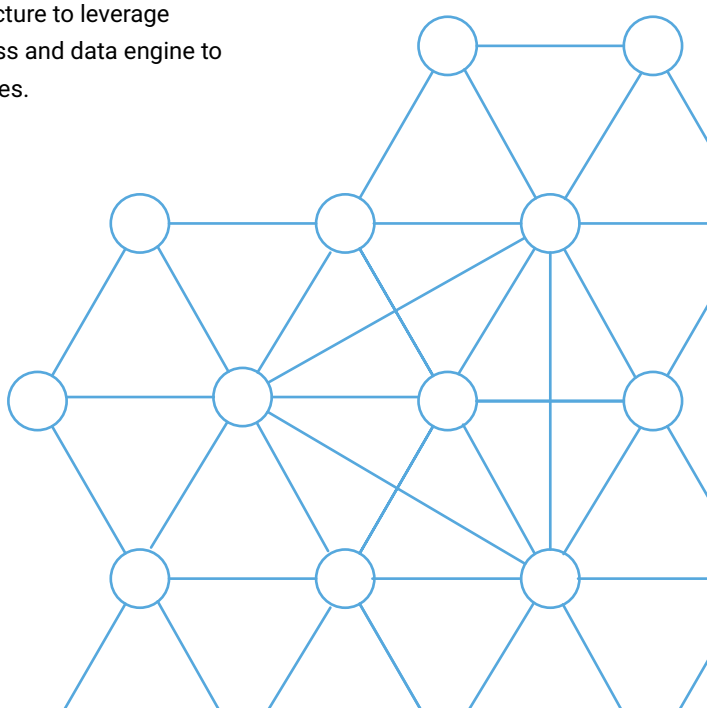
Implement processes to affect the organization's culture, converge and define key GRC program elements and promote risk and compliance awareness of the front line employees.

Implement GRC Program Management

Employ efficient methods to build and execute strategic plans and individual projects and optimize the overall program.

Manage GRC Technology

Establish the infrastructure to leverage technology as a process and data engine to support GRC capabilities.



The Maturity Journey

The Maturity Model for Integrated GRC focuses on building the five levels of capability outlined below over time and implementing the broad strategy as a series of tactical intelligently designed actions.

Siloed
Compliance Driven
Baseline activities are in place to manage risk but are isolated and fragmented

Transition
Activities focused on improving effectiveness are underway to stabilize processes and expand program scope

Managed
Risk Centric
Operational processes have evolved into a steady state and are now effective, repeatable and sustainable

Transform
Transformative initiatives are executed to build better connection between risk management and business

Advantaged
Opportunity Focused
Processes are optimized and balanced by business context and risk priorities

Siloed

The Siloed stage focuses on baseline activities needed to manage risk and is the starting point for all organizations. At this stage the organization is not necessarily deficient in its approach but coordination across functions is very limited.

Managed

The Managed stage depicts the phase at which organizations reach a coordinated, sustainable program. The GRC program, at this point, is effective and achieving its objectives but is still lacking the critical connection to the business that will turn the effort into a valuable contributor to the business strategy.

Transition & Transform

The Transition stage and Transform stage help the organization “move to the next level” with initiatives that evolve critical capabilities and set the stage for advanced capabilities.

Advantaged

The Advantaged stage is designed to be achievable for most organizations. This is not an ‘ideal, pie-in-the-sky’ aspiration but an advanced stage of maturity that optimizes the GRC program. At this point, risk and compliance is part of business operations and the organization reaps the benefits of a coordinated program.

Foundations

Foundations are critical elements necessary for the overall success of the maturity journey for Integrated GRC. Without these foundations in place, the organization will face difficulties throughout the journey based on lack of focus, commitment, resources or strategy. Any organization looking to improve its maturity for Integrated GRC should discuss and address these foundations.

Management commitment

The degree and level of leadership commitment to overall risk and compliance management culture, strategy and priorities should be established as maturing GRC processes takes time and resources.

Performance and acceptable risk

Defined levels of performance and acceptable risk for the business need to be established to set the target state for the GRC program and ensure the business understands the level of effort and benefits involved.

Expectations and measurement

Clear expectations and success criteria defined for the GRC program must be communicated by management to guide strategies.

Stakeholder involvement

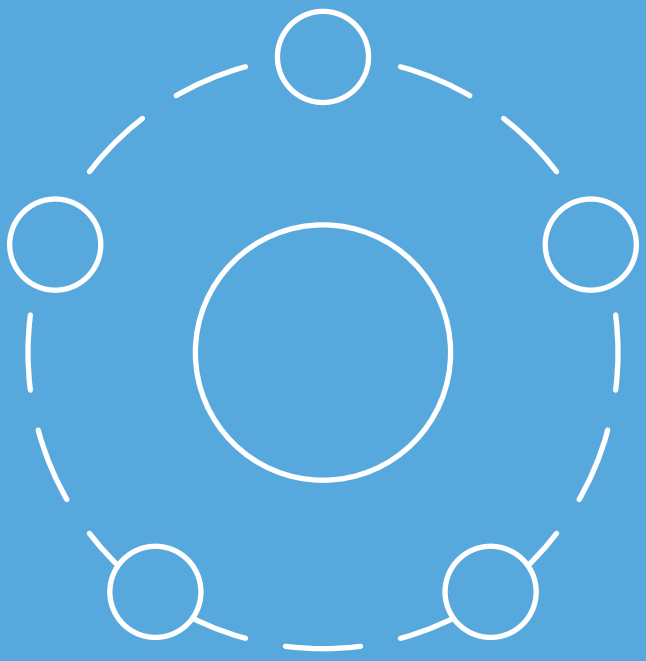
Key business stakeholders and constituents need to agree on the importance of continuous improvement and maturity of GRC processes.

Budget and resources

Sufficient resources for the GRC program must be committed to achieve success.

Siloed

Baseline activities are in place to manage risk but are isolated and fragmented



The Siloed Stage

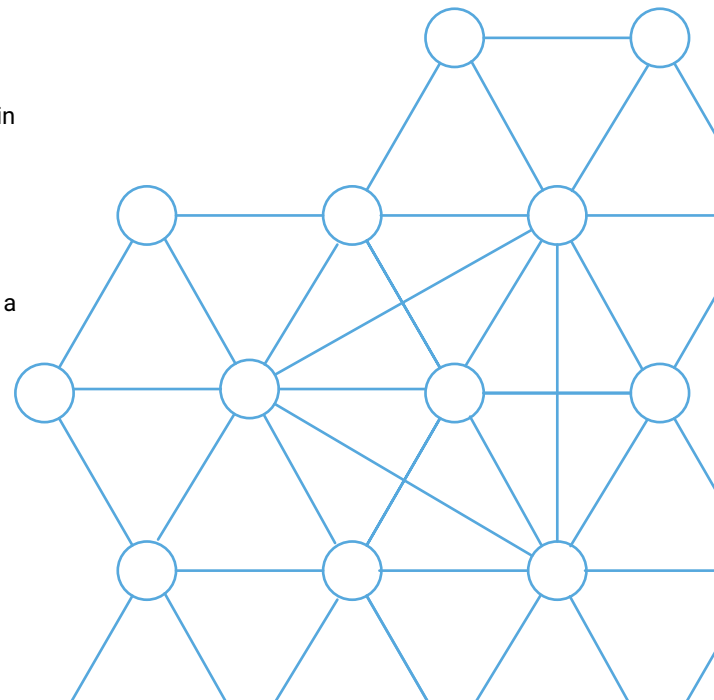
Functional Focus

In the Siloed stage, GRC efforts are focused within the individual functions such as IT, security, finance, business continuity, audit and regulatory compliance. These functions establish their own vision and strategies independently. Ownership of risk and compliance efforts are assigned to the logical management individual. As efforts get underway within that function, governance processes begin to be established. Most functions will require input or partnership with some core service providers or vendors (consultants, advisors, etc.) that help implement processes. Individual engagements with these providers are organized and executed within the functions.

In essence, most of the work at the siloed stage is being coordinated and executed at the 2nd LoD level. Awareness and education processes, such as Security Awareness or Audit training, push requirements to business operations only in the context of the individual domain. Business partners (those operational groups outside the function) have little to no visibility into the 'inner workings' of the functional groups focused on risk and compliance. Domain policies and control structures are established within the function to define requirements that are then pushed down to the 1st LoD. Issues that are identified (risks, control gaps, etc.) are managed independently within the function.

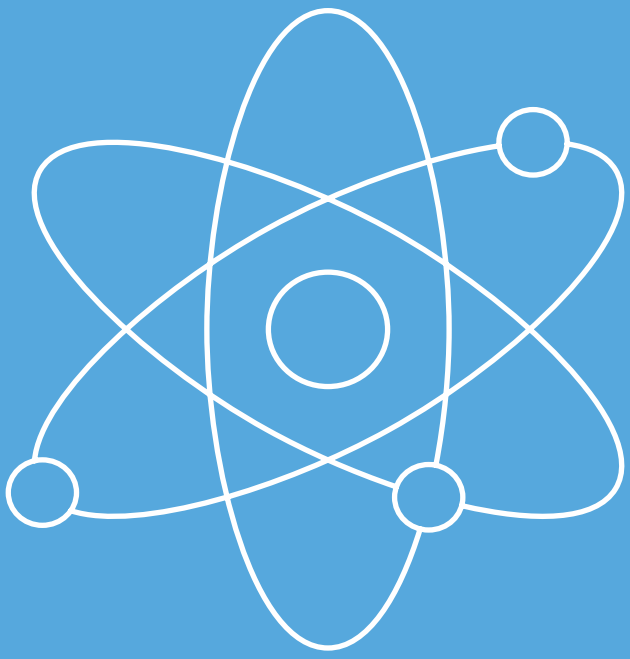
Strategic plans for each domain are built on business cases focused on the individual functional needs. Requirements are defined and resources are designated to implement the plan within the functional group. This plan fuels domain level projects that are tracked and managed using the individual processes within the function.

Finally, technology usage supporting GRC processes may be implemented within the function but are focused solely on meeting the operational requirements of the processes within the domain. Domain level technical expertise around the GRC technologies begins to form. The technology may be desktop tools, home grown systems, commercial products built for niche needs or in some cases GRC technologies, but are only implemented and utilized within the function for a defined set of use cases.



Transition

Activities focused on improving effectiveness are underway to stabilize processes and expand program scope



The Transition Stage

Building for the Future

Within the Transition stage, the GRC program begins the trek towards integration. The motivations for this convergence can be many but most organizations identity at minimum some considerable benefits as the domain level (IT, Finance, Legal, etc.) efforts grow within functional groups. First, executive sponsorship for a more integrated approach begins to take hold. This requires multiple functions to embrace the idea that leveraging processes can lead to greater benefits for all of the GRC efforts. Typically this is fueled by regular communication between functional stakeholders (executive leadership) as the individual domains mature their own processes.

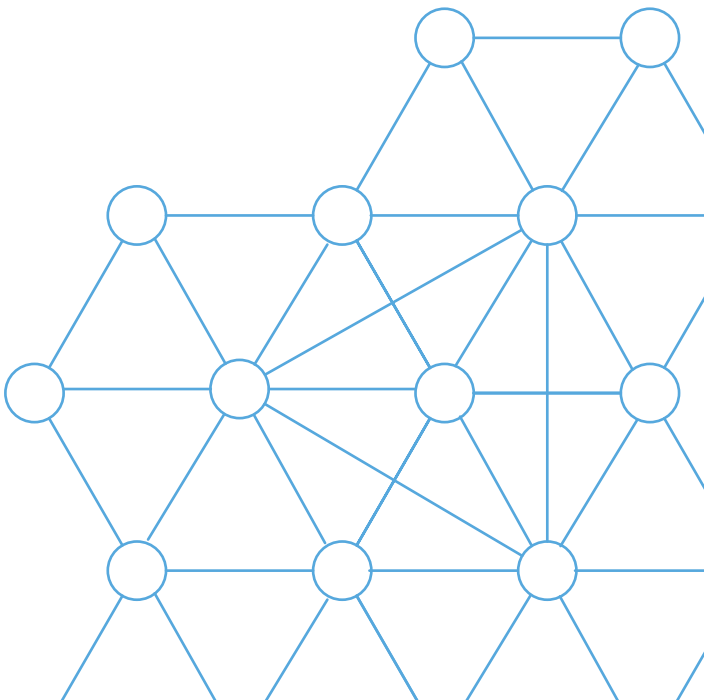
As more and more functional groups begin communicating, awareness starts to build across different domains. This leads to the main GRC functions within each domain to implement an integrated GRC awareness framework for the 2nd LoD. Risk and compliance functional groups within the domains begin to communicate and understand the bigger GRC picture. This awareness strengthens the overall cultural effectiveness of 2nd LoD. Through this communication at the 2nd LoD, certain common elements rise to the surface.

- A common business hierarchy (organizational structure) is required to report risk and compliance issues
- Policies are central to establishing controls and the organization seeks to harmonize and/or standardize policies.
- Issues are a common output of all risk and compliance efforts and need to be reined in to reduce redundant efforts.

These three elements are the first candidates for standardization via taxonomy (structure and definitions) development. Before those taxonomies can be defined and implemented though, a process to develop and maintain GRC related taxonomies must be implemented. Once ownership and accountability for taxonomies is established, taxonomies are developed for business hierarchy, policies and issues.

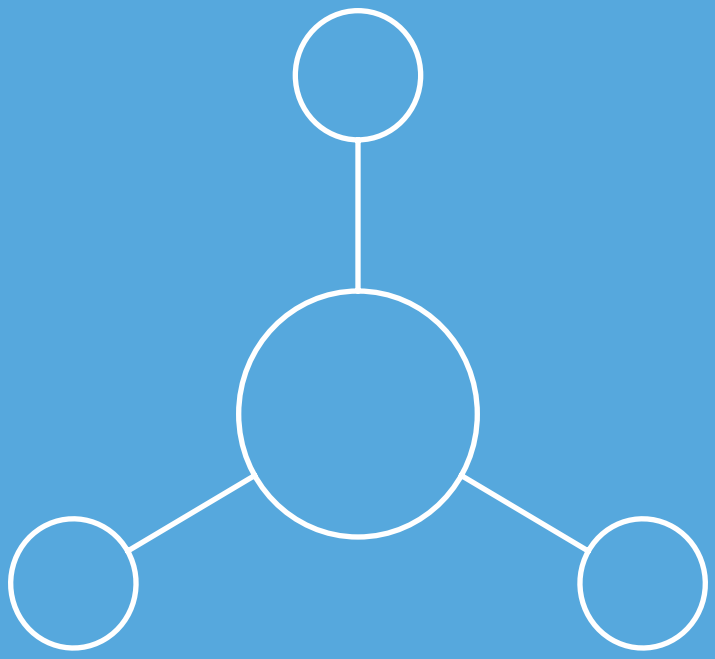
As the executive sponsorship for a coordinated GRC program takes hold and the 2nd LoD builds taxonomies for the basic elements of a GRC program, a long term strategy and roadmap for an integrated program takes shape. Defining this plan is not a one-time effort. However, the Transition phase begins the process. Part of this plan is documenting the existing domain level projects (to identify where each functional group is headed) and cataloging and monitoring domain level metrics (to understand where each functional group is succeeding and struggling). These are key inputs into the next stage of Maturity as the Integrated GRC program strategy emerges.

From a technology perspective, the Transition phase includes activities to catalog the individual domain level technology usage. Tools utilized within each functional group are identified and a technical architecture must be aligned with the taxonomy development for the common elements (business hierarchy, policies, issues). Additionally, most functional groups at this time have been developing technical solutions to solve domain level issues. Implementing (or adopting a standard) Software Development Lifecycle (SDLC) for GRC technology development will ensure future efforts are coordinated and controlled.



Managed

Operational processes have evolved into a steady state
and are now effective, repeatable and sustainable



The Managed Stage

Operationally Sound

The Managed stage represents a significant level of maturity for an organization. An organization that reaches this level has an operationally sound program that is effective and is impacting the organization on a daily basis. Organizations could stay at this level for some time working through the complexities of integrating risk and compliance efforts across multiple functions. However, it is important to acknowledge that while this is a key landmark on the journey it is not the final destination.

Through the efforts of the Transition phase, roles and responsibilities for the GRC program are formalized. Two key pieces in formalizing the GRC program is the charter and establishment of integrated governance structures:

- GRC Program Committee – cross functional management team responsible for moving the overall GRC strategy forward
- GRC Technology Committee – cross functional management team that focuses on the technology infrastructure supporting the GRC Program

As these committees begin working together, oversight coordination across functions improves and leads to the establishment of a decision authority for integrated elements of the GRC Program. This is especially necessary to continue the taxonomy work begun in the Transition phase. Finally, given there is increase cooperation and coordination across functions, external service providers (vendors, consultants, etc.) can be consolidated to focus on Preferred (or strategic) partners.

The next step beyond building a framework for 2nd LoD awareness (established in Transition phase) is a strategy around converging 1st LoD education and training programs. As the GRC program becomes more integrated, the effort to build one view of risk and compliance responsibilities extending to the 1st LoD must be tackled. This is an important milestone in establishing the risk culture of the organization. Another important aspect of promoting risk/compliance principles throughout the organization is to continue the establishment of common taxonomies for GRC elements. In the Managed stage, the organization can now institute taxonomies for Assets (logical and physical, business and IT) and common definitions of Risks and Controls. As continuation of the taxonomy work in the Transition phase (focusing on Policy and Issues), operational processes can now implement those taxonomies to result in integrated Policy Management and Issues Management.

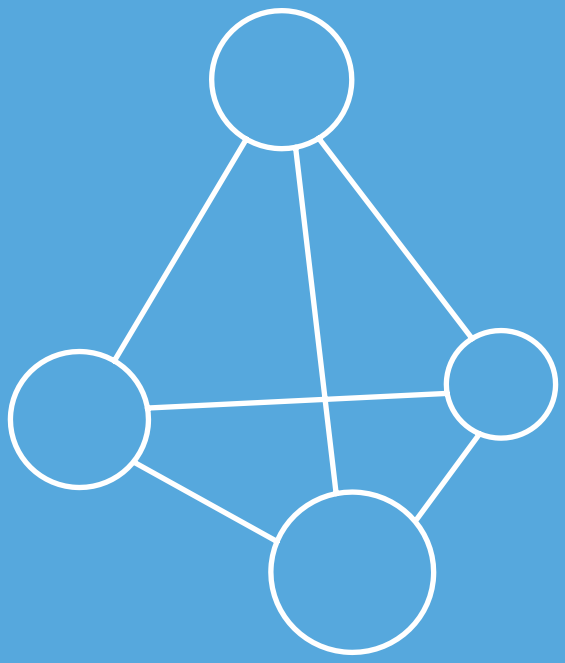
GRC Program Management in the Managed stage has several essential building blocks for the future of the integrated GRC program:

- The strategy and roadmap documented in the Transition Phase takes shape in the form of key objectives and outputs, technical requirements and resource requirements. The strategy can be analyzed by the individual functions to make adjustments to domain processes, fit into the bigger picture and drive a stream of projects to break down the silos.
- Projects become more complex with connections between functions and therefore require more oversight and management. A Project Management Office (PMO), in many cases, is required to provide the coordination or reporting. Additionally, projects will need a prioritization model to ensure projects are executed in the proper sequence.
- Finally, the program will need metrics to identify key milestones and critical junctures. Metrics will also be used later to optimize the program. As the integration activities are getting underway, it is recommended to establish some standardized metrics to monitor.

In the Transition stage, technology usage has been cataloged and a technical architecture has been outlined that aligns with the ongoing taxonomy work. In the Managed stage, this results in a migration or integration of GRC technologies. This work will be built upon a consolidated data architecture and an integrated technology architecture. In some cases, domain level tools (spreadsheets, homegrown tools, etc.) may be eliminated as a larger, integrated GRC infrastructure is built. During this process, common technical implementation practices should be followed. Finally, this evolution of the technical infrastructure will require proper resources. A formalized integration development team and technical support team will be necessary to ensure successful technology projects.

Transform

Transformative initiatives are executed to build better connection between risk management and business



The Transform Stage

Communication & Stabilization

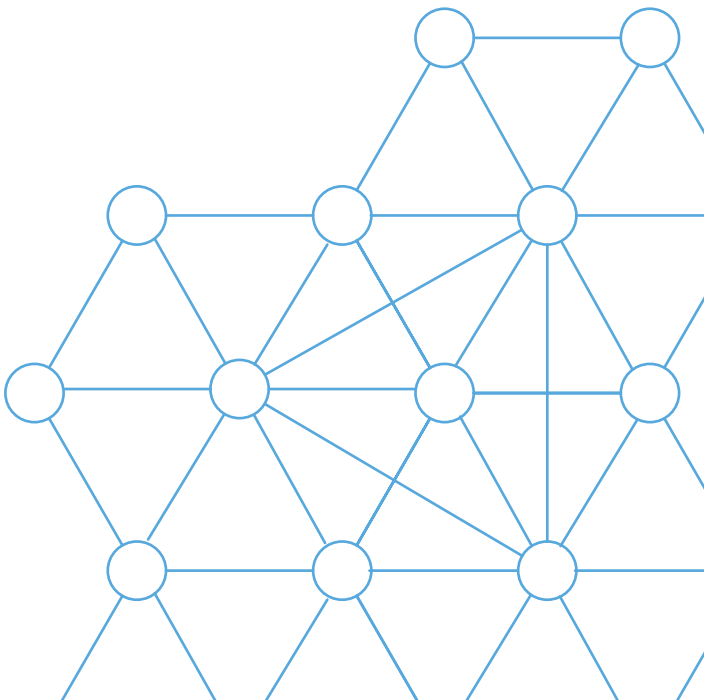
The Transform Stage focuses on building for and more meaningful communication across the program. The Managed Stage represents much work. As that work becomes more confirmed and proven, the momentum towards integration can cause logjams in priorities and resource crunches. The Transform Stage is important to stabilize the efforts and ensure the organization is seeing the value that is expected out of the GRC Program.

Since the major governance committees were established in the Managed stage, within the Transform stage these bodies move into an operational state as a recognized, informed management team with a regular cadence of governance activities. Examples of these activities include supporting and sponsoring the taxonomy work, coordinating the technical implementations and prioritization of projects. Additionally, these bodies will be the faces of the program as key representatives for communicating progress to executive management and other functional leadership.

The cultural impacts of the integrated GRC program will be manifested in a more cohesive awareness program for the organization. Testing processes to ensure the awareness and integration of risk/compliance priorities and responsibilities for the 1st LoD will improve overall acceptance and accountability. Additionally, the taxonomy work in the Managed Phase will need to be implemented. Since Assets, Risks and Controls are fundamental pieces for all risk and compliance processes, the Transform Stage signifies a substantial shift in how processes work together. With common taxonomies defined for these core elements, the organization can implement integrated asset management, control assessment and risk assessment processes. Processes may not be completely combined or consolidated but at a minimum the organization is describing those components (assets, risk and controls) using a common language. The impact to reporting GRC Issues can be greatly improved simply through this mutual vernacular.

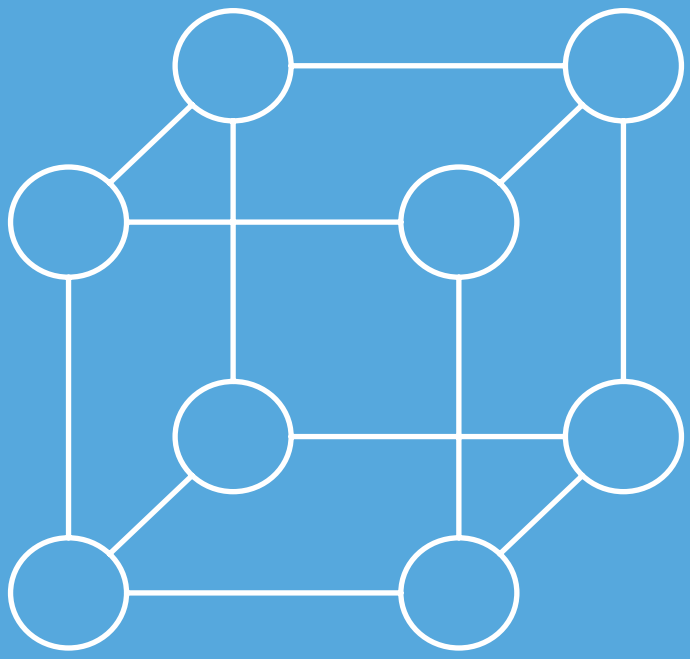
The Program Management elements in the Transform stage also focus on rigor, consistency and cadence. The PMO (or equivalent body) will have multiple work streams to accomplish in the Managed Stage. In the Transform stage, a regular cadence of oversight meetings will be driven by the review and monitoring of metrics produced by the implementation projects. These metrics will identify gaps and stimulate improvement plans that must be fed back into the project funnel.

From a technology perspective, the Transform stage represents a move to a truly managed and operational infrastructure. This requires implementing the operational model (chargeback or cost sharing depending on the general IT models of the organization). Regular healthchecks and metrics on the technology should be conducted as the program will continue to onboard processes, functions and other data stores as the program moves forward. This also requires more rigor around managing incoming requests (for modifications to existing processes, for onboarding new processes, etc.) and a change management program that is controlled and prioritized.



Advantaged

Processes are optimized and balanced by business context and risk priorities



The Advantaged Stage

Program Optimization

In the final stage, the organization pulls together the substantial pieces into an Advantaged state. The Advantaged stage is highlighted by the fact that GRC processes are deeply aligned with business needs, objectives and strategies. The ultimate goal of the GRC Program - termed Risk Intelligence within the Maturity Model structure - is a multi-dimensional understanding of risk, visibility across issues and a coordinated risk and compliance program that is a competitive advantage for the enterprise.

At this point, the governance structures of the program can address onboarding new functional groups into the broader strategy. The training for both 1st and 2nd LoD employees has built a risk-aware and educated workforce. Taxonomy development for other types of GRC elements (incidents, regulatory obligations, crises, etc.) can be prioritized and implemented to gain even more consistency across the organization. The key development during this stage - since functional groups are using common taxonomies for risk, controls and assets - is a truly integrated view of risk that can drive prioritization based on business impacts. An integrated risk prioritization process can be implemented where risks can be identified, assessed, treated and monitored using a shared measurement.

Program Management in the Advantaged stage can utilize the integrated nature of projects and strategies to optimize and rationalize the financial investments in GRC. Ongoing strategy management includes regular planning and monitored execution. Given the program has been executing for a period of time, benchmarking against peers and industry can be conducted and will provide insight on the program. This, and the established metrics within the program, can help fuel a continuous improvement model.

Finally, the technology infrastructure will reach an operational, steady state where changes in the program are driving changes in the technical operations. This will include managing the data integrations between systems of record and maintaining a backlog and roadmap for technical requirements. Many organizations at this stage establish a GRC Technology Center of Excellence with dedicated technical resources that partner with the functional teams and business to implement systems in support of the program.

CONCLUSION

Implementing an Integrated GRC program is not a simple task. Most organizations build siloed functional programs first. To date, only those organizations that realize Integrated GRC is an opportunity to transform risk into a competitive advantage, or ones that have suffered substantial negative impact from realized risks or compliance enforcement, have aggressively sought to mature their GRC programs. Now, however, the velocity of growth in compliance requirements and exponential expansion of risk affects every company. The need for Integrated GRC has never been greater.

Companies in the **Siloed** stage must ensure their individual functions are responding to risk and compliance drivers effectively first. Before any integrated activities can take place, at a minimum, key functions need to understand their role in managing risk and meeting compliance requirements. In order to move from Siloed to Managed stages, organizations **Transition** through projects that catalog and organize GRC efforts and build the business case to take GRC to the next level. Companies in the **Managed** stage see much better visibility into risk and compliance issues through communication between executive stakeholders and GRC executors, common taxonomies for the basic elements of GRC and an integrated technology strategy. In order to reach the Advantaged stage, GRC processes **Transform** through more rigor and a regular cadence of governance activities, taxonomy implementations and monitoring metrics to identify where the program is working effectively and where gaps still need to be addressed. This allows the organization to harmonize GRC efforts across business requirements and reduce administrative overhead and costs. Organizations in the **Advantaged** stage are ready to realize the competitive advantage of harnessing risk such as beating competitors to market, launching new products and services with calculated efficiencies and avoiding major issues that affect reputation and the bottom line. Organizations in this final phase speak risk in the "business' language" and are able to identify and respond to emerging business requirements ahead of the curve using a well-oiled integrated GRC program.

OCEG®

Driving Principled Performance®

www.oceg.org